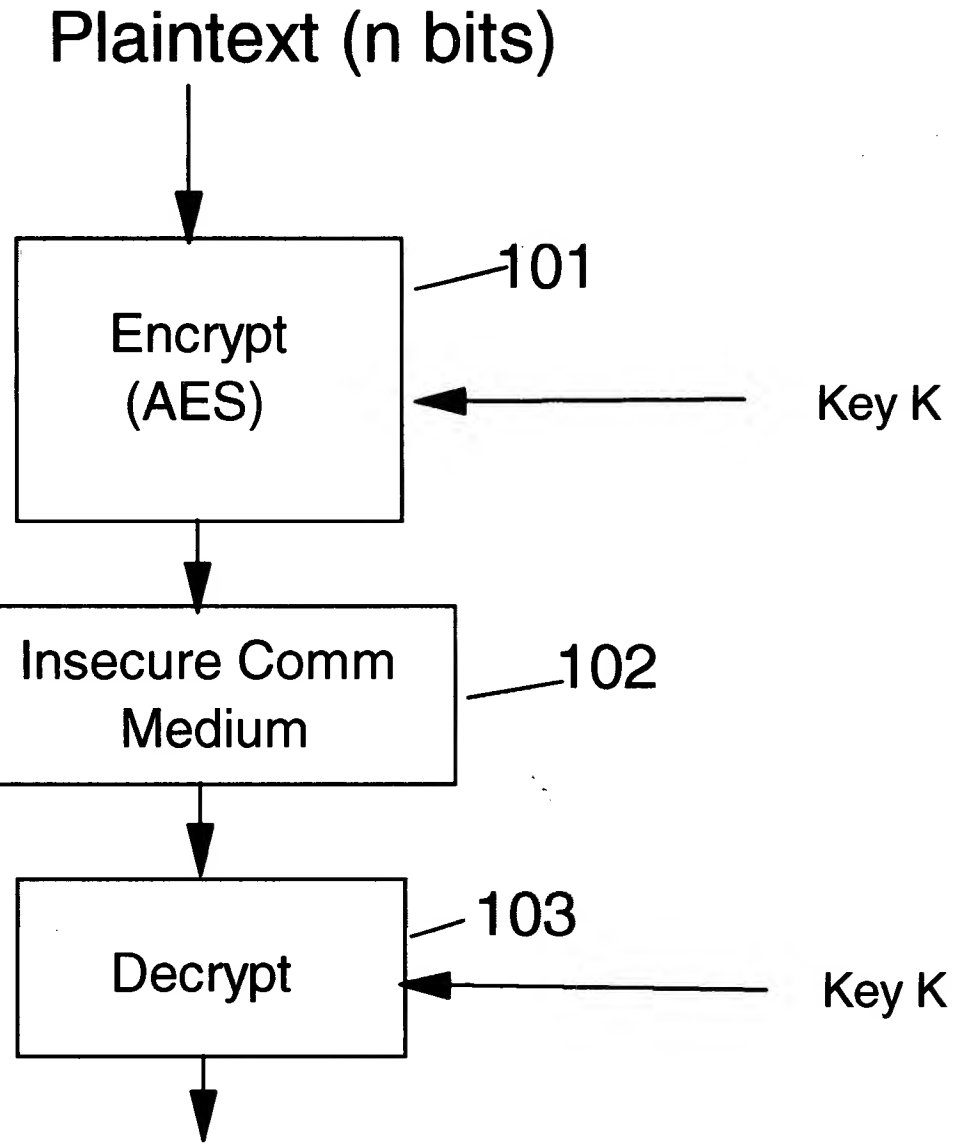
Plaintext (n bits)
Encrypt
(AES)
101
Key K
Insecure Comm
Medium
102
Decrypt
103
Key K

Fig. 1

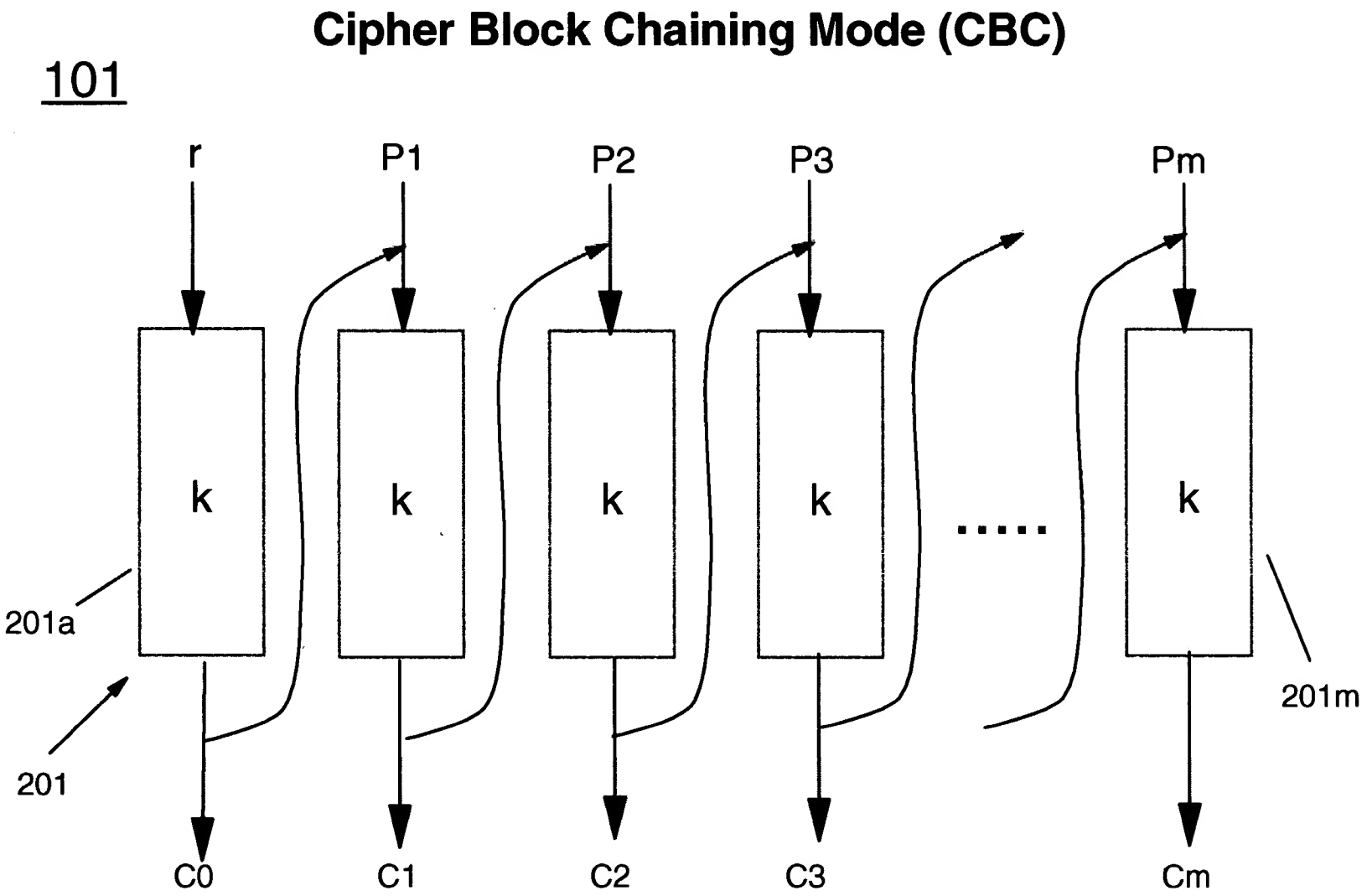
Cipher Block Chaining Mode (CBC)
101
r
P1
P2
P3
Pm
k
k
k
k
k
201a
201
201m
C0
C1
C2
C3
Cm

Fig. 2

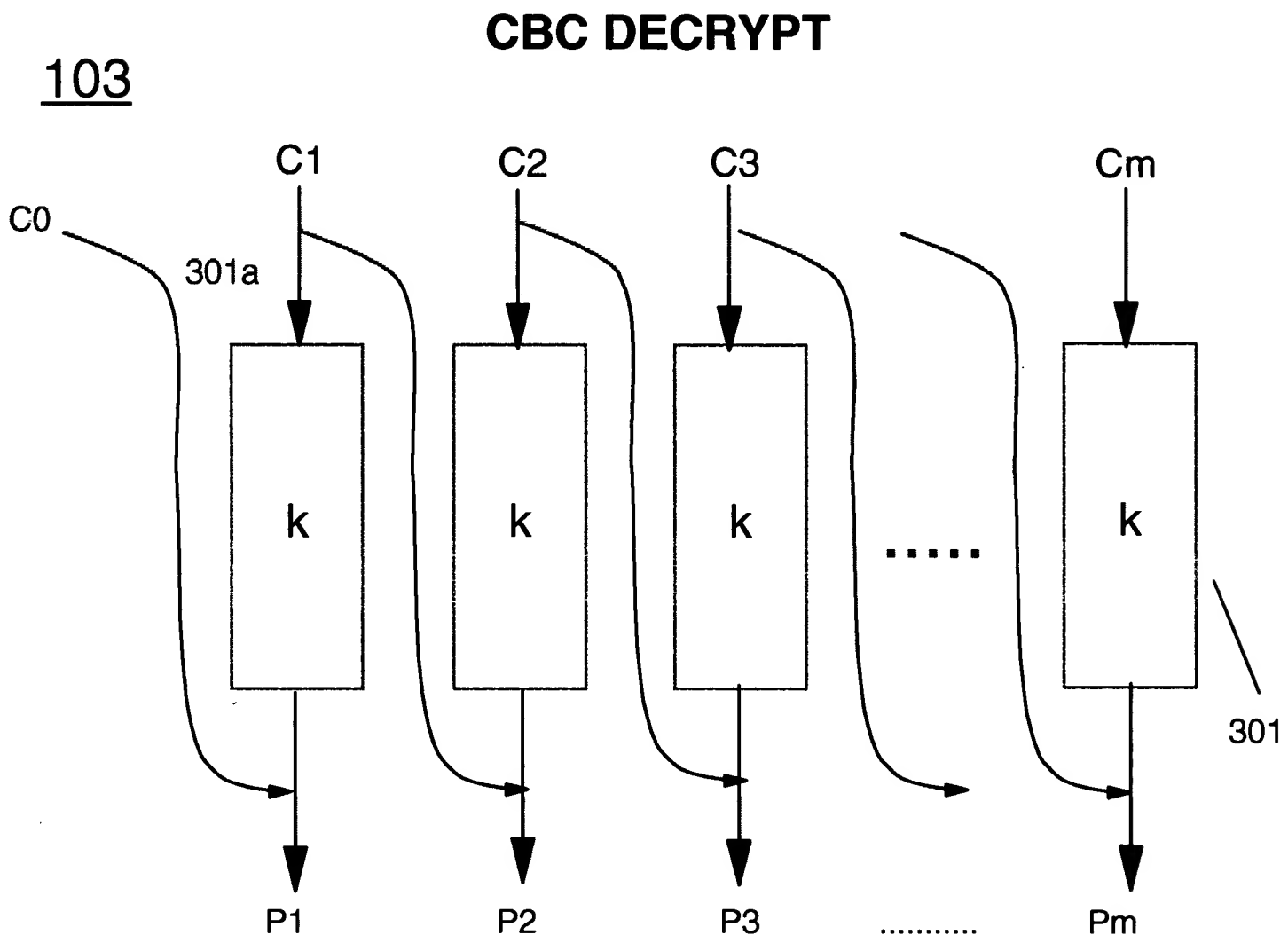

Fig. 3

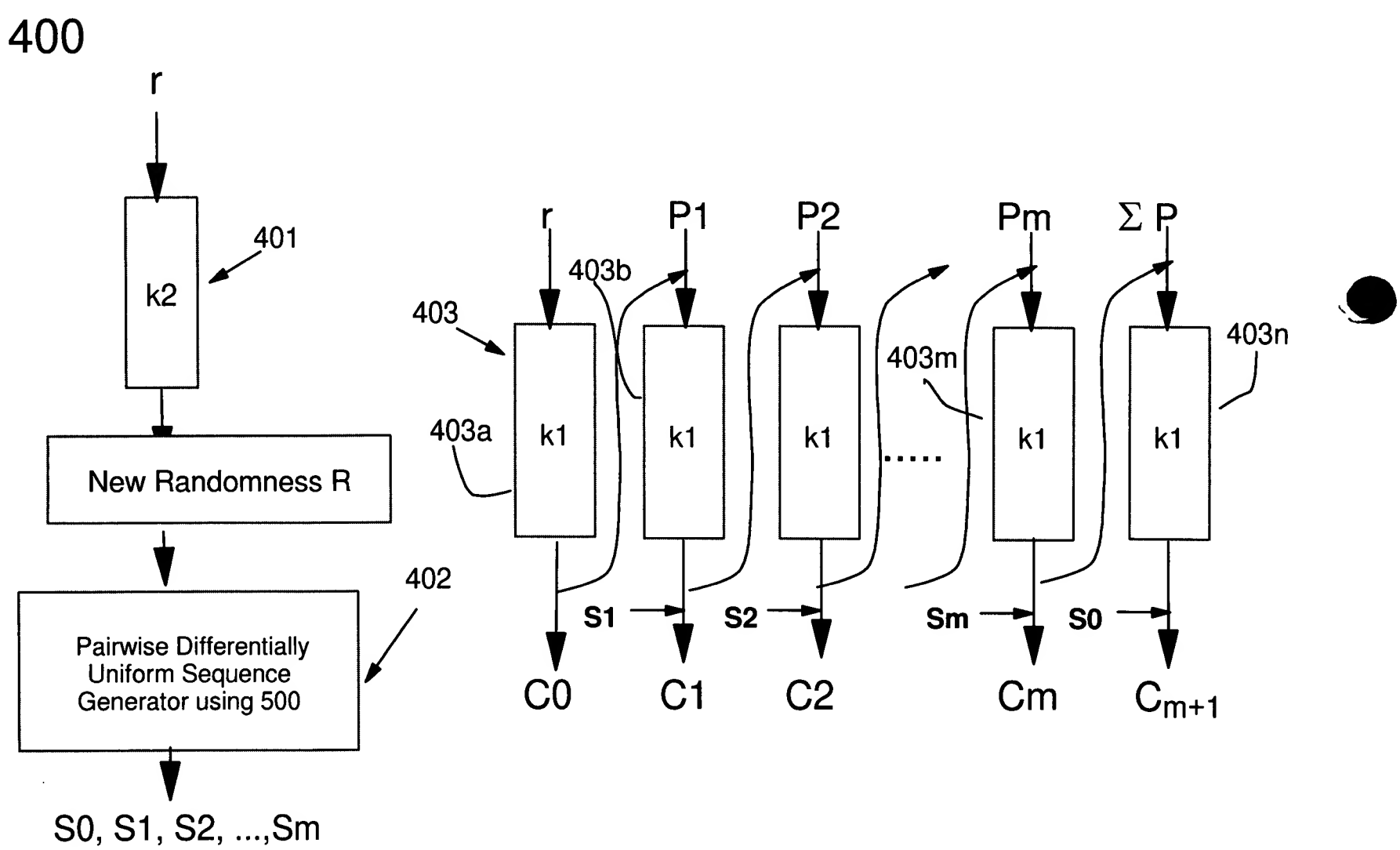
400
r
401
k2
New Randomness R
402
Pairwise Differentially Uniform Sequence Generator using 500
S0, S1, S2, ...,Sm
r
P1
P2
Pm
Σ P
403b
403
403a
403m
403n
k1
k1
k1
k1
k1
S1
S2
Sm
S0
C0
C1
C2
Cm
Cm+1

Fig 4

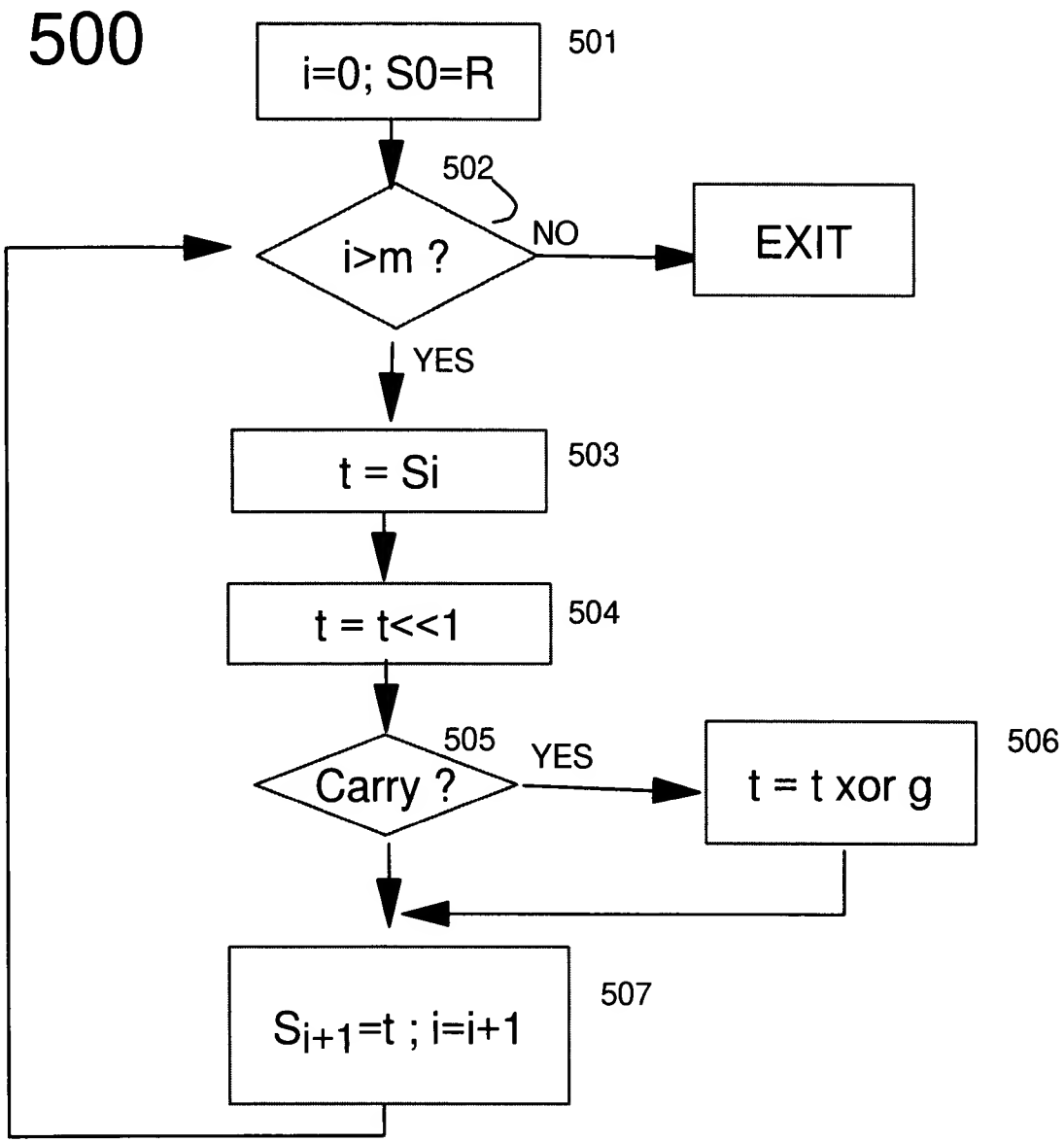
500
i=0; S0=R
501
502
i>m ?
NO
EXIT
YES
t = Si
503
t = t<<1
504
505
Carry ?
YES
t = t xor g
506
S_{i+1}=t ; i=i+1
507

Fig 5

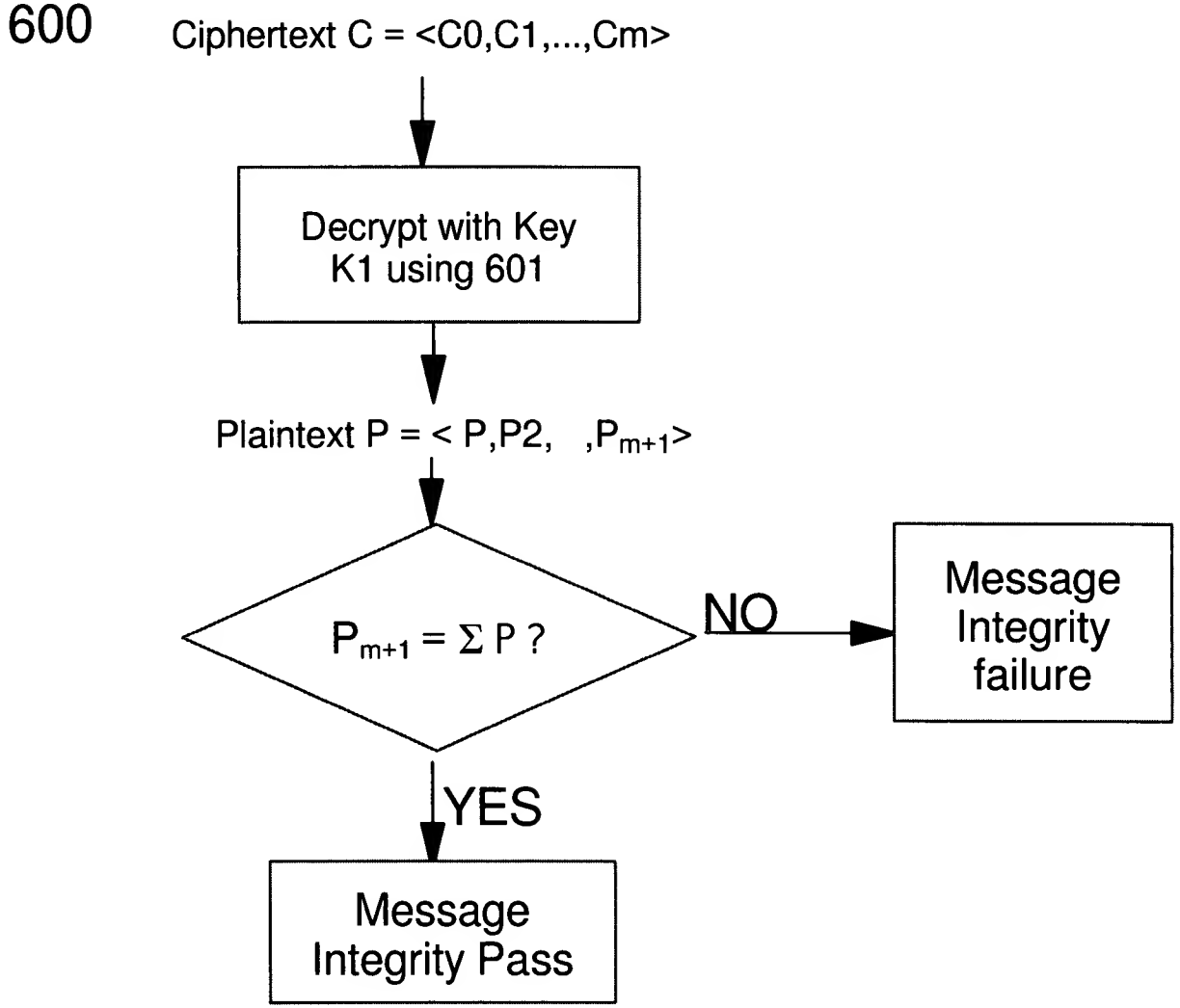
600
Ciphertext C = <C0,C1,...,Cm>
Decrypt with Key K1 using 601
Plaintext P = < P,P2, ,Pm+1>
Pm+1 = Σ P ?
NO
Message Integrity failure
YES
Message Integrity Pass

Figure 6

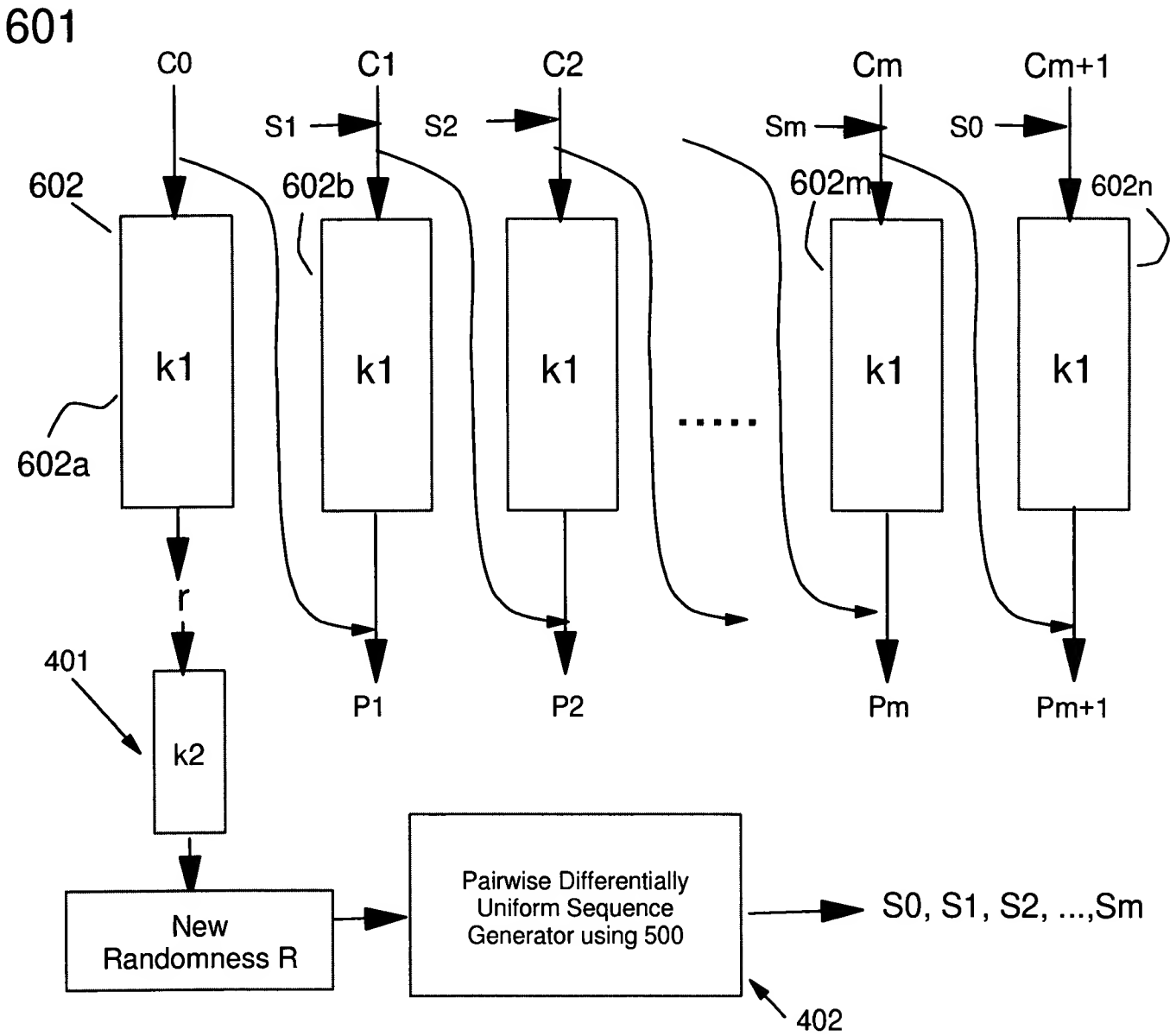
601
C0
C1
C2
Cm
Cm+1
S1
S2
Sm
S0
602
602b
602m
602n
k1
602a
r
401
k2
P1
P2
Pm
Pm+1
New Randomness R
Pairwise Differentially Uniform Sequence Generator using 500
S0, S1, S2, ...,Sm
402

FIG 7

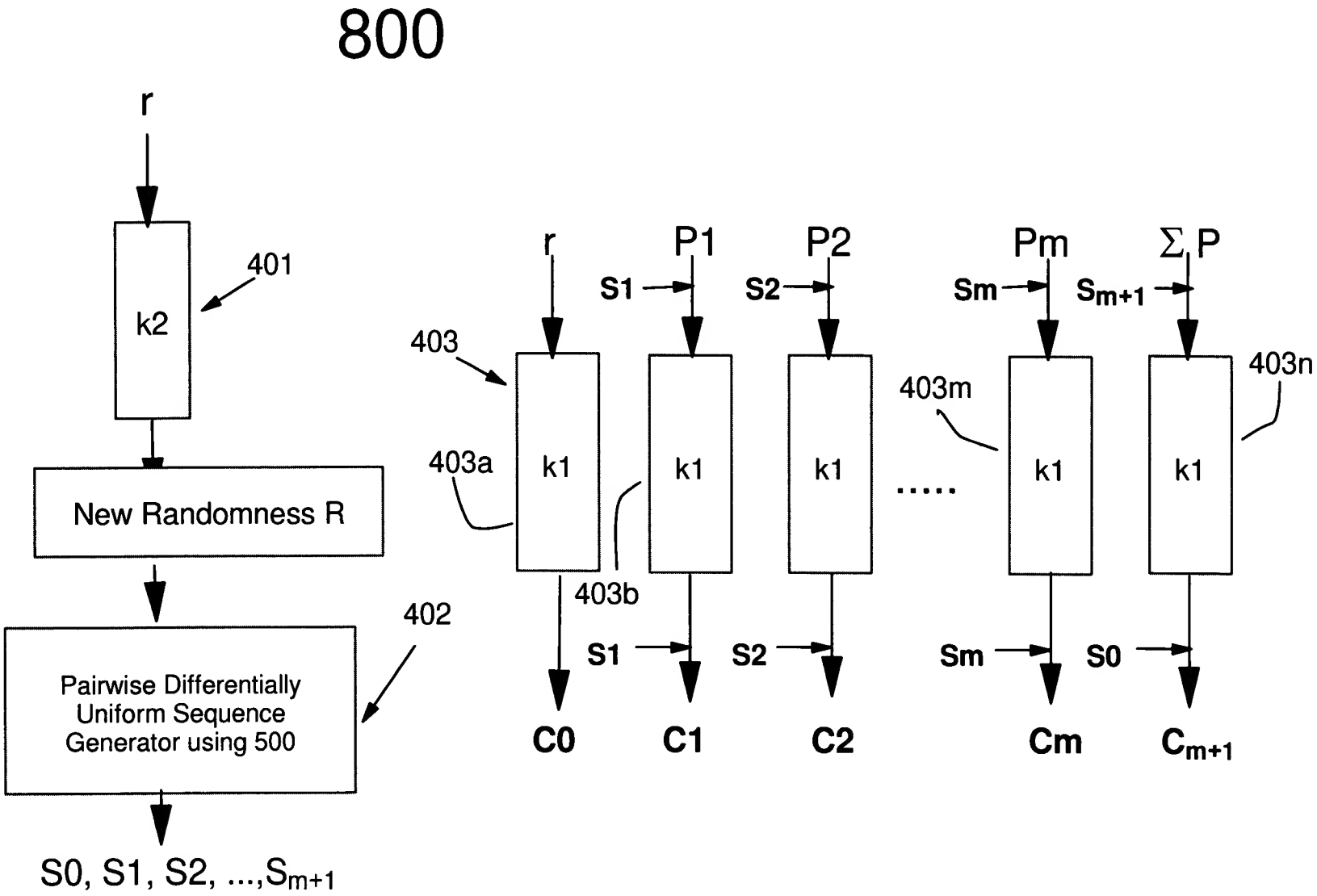
800
r
401
k2
New Randomness R
402
Pairwise Differentially Uniform Sequence Generator using 500
S0, S1, S2, ...,Sm+1
r
P1
P2
Pm
Σ P
S1
S2
Sm
Sm+1
403
403a
403b
403m
403n
k1
k1
k1
k1
k1
.....
S1
S2
Sm
S0
C0
C1
C2
Cm
Cm+1

Fig 8

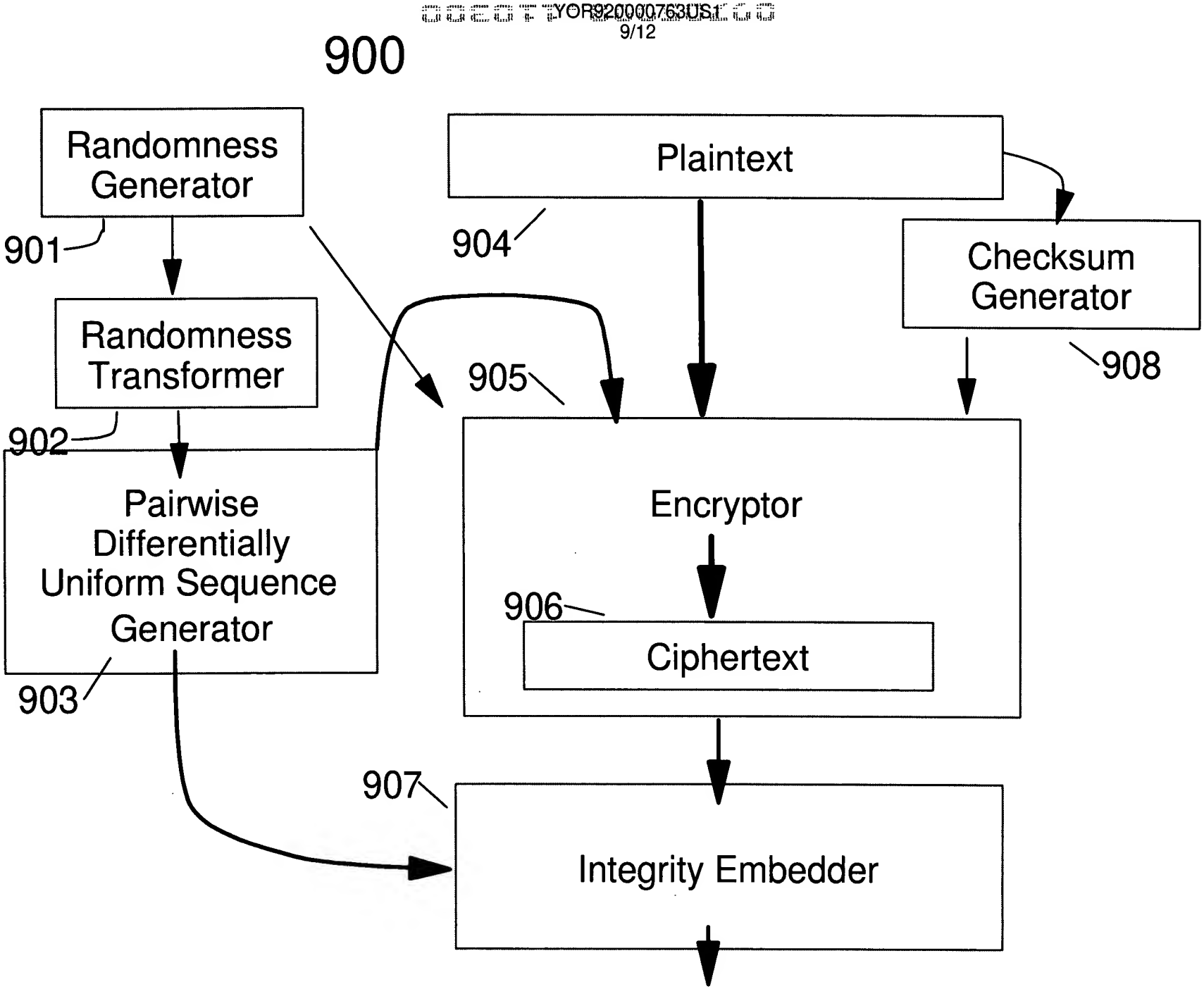
900
Randomness Generator
901
Randomness Transformer
902
Pairwise Differentially Uniform Sequence Generator
903
Plaintext
904
Checksum Generator
908
905
Encryptor
906
Ciphertext
907
Integrity Embedder

Fig 9

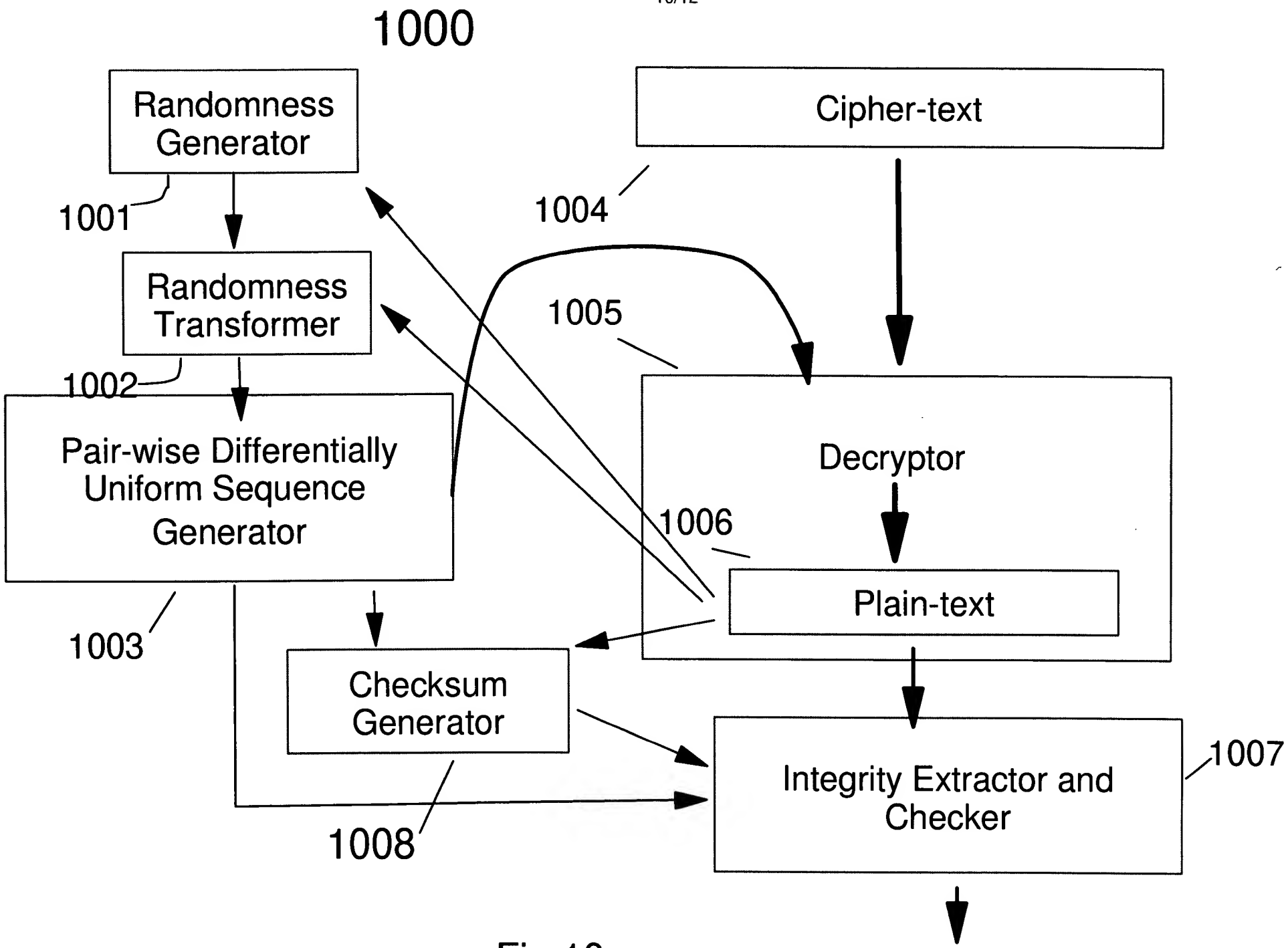
1000
Randomness Generator
1001
Randomness Transformer
1002
Pair-wise Differentially Uniform Sequence Generator
1003
Cipher-text
1004
1005
Decryptor
1006
Plain-text
Checksum Generator
1008
Integrity Extractor and Checker
1007

Fig 10

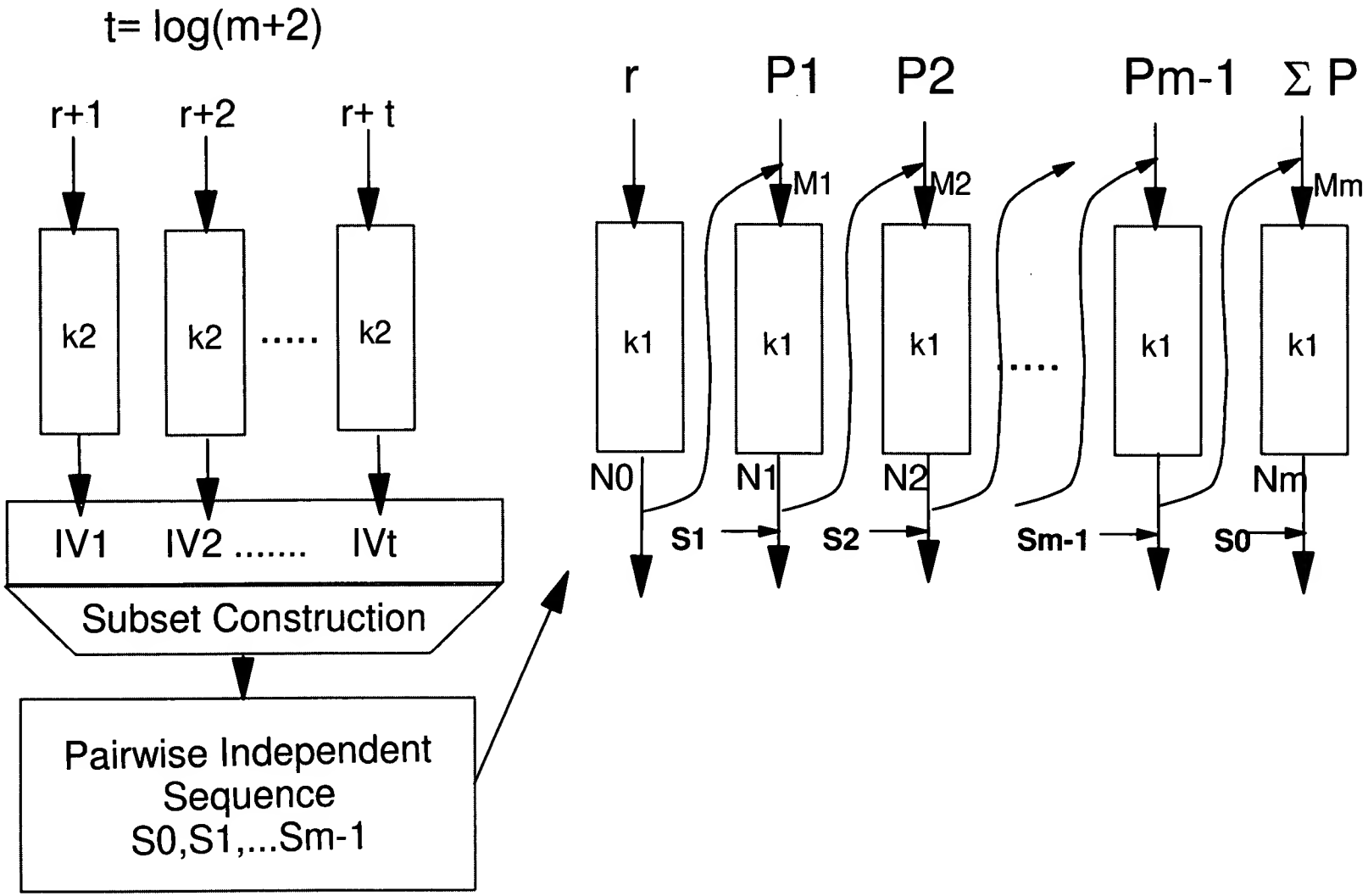
t= log(m+2)
r+1
r+2
r+ t
k2
k2
.....
k2
IV1
IV2 .....
IVt
Subset Construction
Pairwise Independent
Sequence
S0,S1,...Sm-1
r
P1
P2
Pm-1
Σ P
M1
M2
Mm
k1
k1
k1
....
k1
k1
N0
N1
N2
Nm
S1
S2
Sm-1
S0

Fig 11

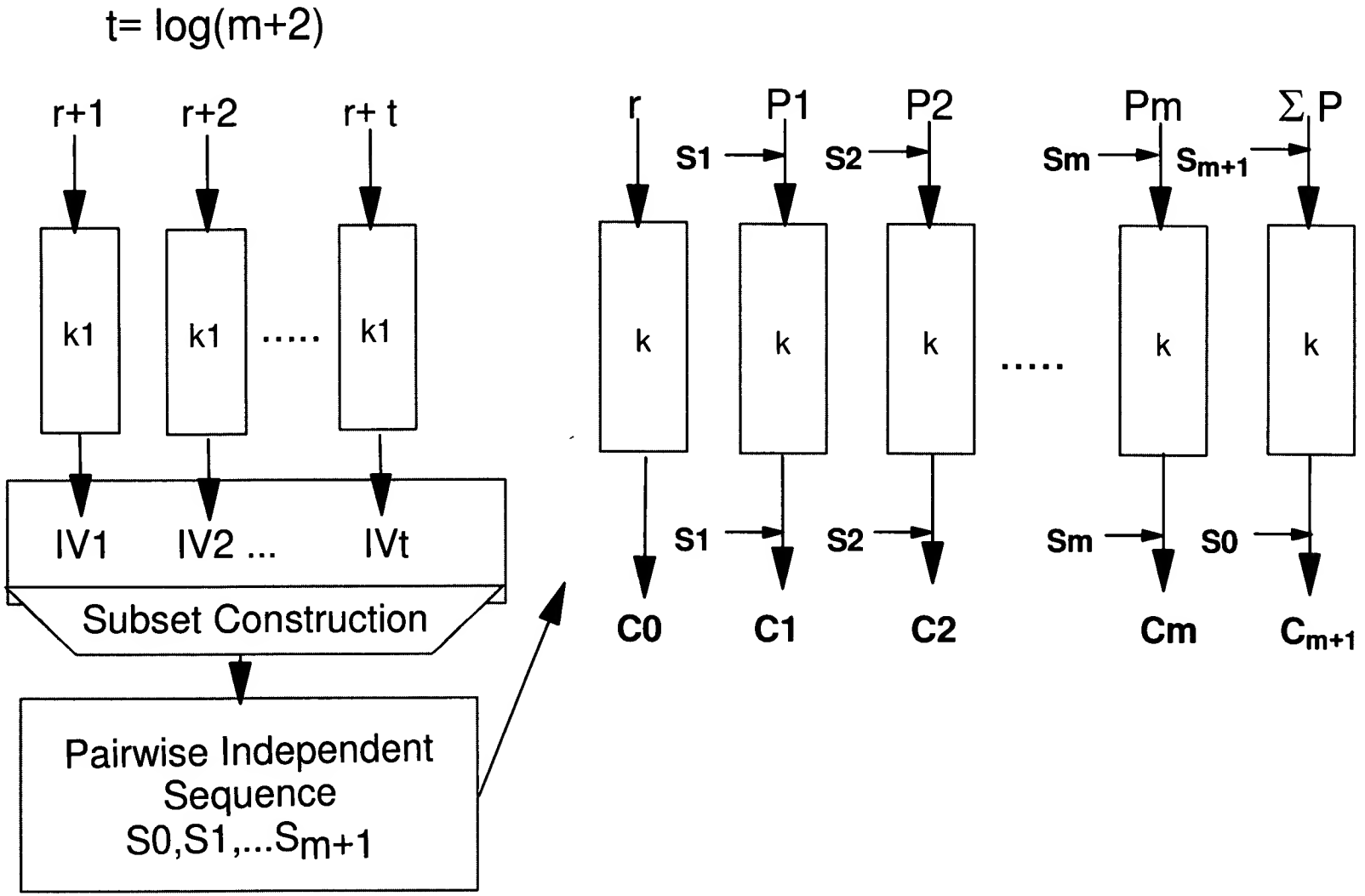
t= log(m+2)
r+1
r+2
r+ t
k1
k1
.....
k1
IV1
IV2 ...
IVt
Subset Construction
Pairwise Independent Sequence
S0,S1,...Sm+1
r
P1
P2
Pm
Σ P
S1
S2
Sm
Sm+1
k
k
k
.....
k
k
S1
S2
Sm
S0
C0
C1
C2
Cm
Cm+1

Fig 12